UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/672,184	09/25/2003	Eduard K. de Jong	SUN-040027	9837

24209 7590 08/29/2008

GUNNISON MCKAY & HODGSON, LLP
1900 GARDEN ROAD
SUITE 220
MONTEREY, CA 93940

EXAMINER	
PICH, PONNOREAY	
ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
08/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/672,184
Filing Date: September 25, 2003
Appellant(s): DE JONG, EDUARD K.

Forrest Gunnison (Reg. no. 32,899)
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 6/30/08 appealing from the Office action mailed 11/26/07.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is substantially correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

US 7,170,999	Kessler et al	1-2007
US 6,789,177	Okada	9-2004
WO 02/079955	Shen Orr	10-2002
US 2002/0120854	LeVine et al	8-2002

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-4, 6-9, 11-14, and 16-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kessler et al (US 7,170,999) in view of Okada (US 6,789,177) in further view of Shen Orr (WO 02/079955) in further view of LeVine et al (US 2002/0120854).

As per claim 1, Kessler discloses receiving a reference to a decryption algorithm and a first cryptographic key and creating a key decryption program (i.e. proprietary client software having embedded decryption algorithms) comprising an instruction stream, said key decryption program configured to perform said decryption algorithm for said first cryptographic key (col 8, lines 50-67 and col 10, lines 58-67). *A person skilled in the art should understand that all programs start out as source code and when the source code is compiled, the resulting software contains instruction streams. The cited portion of Kessler discloses of a proprietary client software received by the client. The proprietary software contains decryption algorithms used to access the encrypted data files via keys SK2 and TK. The fact that the proprietary software exists implies that a reference to a decryption algorithm (i.e. decryption algorithm source code) was received and used to create the proprietary software. According to the cited portion in column 8, the keys used in the decryption algorithm are obfuscated and/or encrypted in the proprietary software. This implies that when the proprietary software was created, not only was the source code to the decryption algorithm received, but also the first decryption key, i.e. SK2, which is used to decrypt TK.*

Kessler discloses applying a cryptographic process to a second cryptographic key, i.e. TK, to create an encrypted second cryptographic key wherein said cryptographic process receives a public key and second cryptographic keys as inputs (col 5, lines 29-42). *Note that TK is encrypted using PK2, which implies that both TK and PK2 were inputs to a cryptographic process.*

Kessler discloses sending said key decryption program (col 4, lines 44-46 and col 8, lines 50-51).

It is noted that in Kessler's invention, a public key PK2 is used to encrypt the second cryptographic key, i.e. TK, while a secret key SK2 is used to decrypt the second cryptographic key. In the invention recited in claim 1, a first cryptographic key is used to both create the encrypted second key and to decrypt the second key, i.e. perform said decryption algorithm for said first cryptographic key. However, Okada discloses using a first cryptographic key, i.e. session key, to both encrypt and decrypt a second key, i.e. content key (col 9, lines 21-26 and col 10, lines 39-53). Note that the content key disclosed by Okada is equivalent to the track key (TK) disclosed by Kessler.

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Kessler's invention such that rather than use an asymmetric key system to encrypt/decrypt the second cryptographic key TK, a symmetric key system was utilized such that a first cryptographic key was used to both encrypt and decrypt the second cryptographic key as per Okada's teachings. One skilled would have been motivated to do so because symmetric key systems are faster and less computationally intensive than asymmetric key systems. Another rationale for why it would have been obvious to modify Kessler's invention in the manner discussed using Okada's teachings is that the simple substitution of Okada's key encrypting key methodology within Kessler's invention would do no more than yield the predictable result of a track key (TK) being encrypted and decrypted using a single first cryptographic key rather than use of an asymmetric key pair to encrypt and decrypt TK.

Kessler also does not explicitly disclose scrambling, said encrypted second cryptographic key into said instruction stream using a code obfuscation method indicated by an obfuscation descriptor,

said scrambling creating an obfuscated key decryption program, said obfuscation descriptor based at least in part on a target ID wherein said target ID specifies a user device for executing an obfuscated application program. Kessler does not disclose the key decryption program that was sent is obfuscated. Kessler does not explicitly disclose the receiving, creating, applying, scrambling, and sending step were all done on the same application program provider.

However, Shen Orr discloses creating an obfuscated key decryption program (p16, line 31-p17, line 3; p21, lines 1-2; and p24, lines 17-19) via use of an obfuscation method indicated by an obfuscation descriptor (p9, lines 19-24 and p9, line 33-p10, line 2), said obfuscation descriptor based at least in part on a target ID wherein said target ID specifies a user device for executing an obfuscated application program (p9, line 33-p10, line 2). *Note that in the cited portions of Shen Orr, several techniques are used to secure a key decryption program, including use of one or more obfuscation methods to render the decryption program obfuscated. The obfuscation method is chosen based on at least one variable parameter which is partially determined by the hardware or software identifier of the end user device—i.e. the target ID.*

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Kessler's invention using Shen Orr's teachings by obfuscating Kessler's proprietary client software before sending it to the client via an obfuscation method indicated by an obfuscation descriptor that is based at least in part on a target ID (i.e. the end user's device's hardware or software identifier) that specifies a user device for executing an obfuscated proprietary client software. One skilled would have been motivated to do so because as recognized by Shen Orr, there was a need in the art to provide variable security mechanisms (p6, lines 20-26), which would provide more security than using a single security scheme such as the one used by Kessler.

Shen Orr also does not disclose that the obfuscation method involves scrambling said encrypted second cryptographic key into said instruction stream. However, LeVine discloses of an obfuscation method which involves scrambling an encrypted key into the instruction stream of a program (paragraphs 12, 21, 23, 26 and 78).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to further modify Kessler's invention such that the obfuscation method used involves scrambling said encrypted second cryptographic key into said instruction stream. The rationale for why it is obvious is that as per Shen Orr's teachings, obfuscation to secure a program was already used in Kessler's modified invention and the substitution LeVine's obfuscation method in place of one of the obfuscation methods used by Shen Orr would do no more than yield the predictable result of obfuscation as per LeVine's methodology.

As per the limitation that the receiving, creating, applying, scrambling, and sending step were all done on the same application program provider, note that in Shen Orr invention, all the steps of creating an application program to be sent to an end user is performed on a single application builder 102 (Fig 1 and Fig 4A-4B). At the time applicant's invention was made it would have been obvious to one of ordinary skill in the art to have the combination invention of Kessler, Okada, Shen Orr, and LeVine perform all the steps of application program obfuscation on a single application program provider, i.e. application builder. One skilled would have been motivated to do so because it would lessen the chances that someone would obtain the key decryption program before it was secured using Kessler's modified invention.

Claims 6, 11, and 16 recite similar limitations as what is recited in claim 1 and are rejected for similar reasons. Note that Kessler, Okada, Shen Orr, and LeVine's inventions are all performed using

computers. All computers contain a processor and a memory, coupled to the processor, having stored therein computer readable instructions that are executed by the processor to perform a method according to the instructions.

Claims 2, 7, 12, and 17:

Kessler further discloses method, medium, means, and apparatus for sending digital content protected by said second cryptographic key (Fig 2 and col 10, lines 58-67).

Claims 3, 8, 13, and 18:

As per claims 3, 8, 13, and 18, Shen Orr further discloses sending said obfuscated key decryption program together with said digital content (p19, line 32-p20, line 8).

Claims 4, 9, 14, and 19:

As per claims 4, 9, 14, and 19, Kessler does not explicitly disclose wherein said target ID comprises a VM ID. However, Shen Orr discloses target ID icluding a software identifier (p10, lines 1-2). Further, official notice is taken that virtual machines having VM ID were well known in the art at the time applicant's invention was made. At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to have the target ID comprise VM ID. One skilled would have been motivated to do so because as disclosed by Shen Orr, software ID could be utilized as a target ID and because virtual machines were known types of software, using the VM ID as a target ID would do no more than yield a predictable result of using a specific type of software ID as the target ID.

(10) Response to Argument

Before addressing appellant's arguments, a few preliminary matters are addressed. First, it is noted that appellant had filed IDS's after Final rejection was made for the current application. The

IDS's submitted on 4/21/08 and 6/19/08 are placed in file, but the documents listed therein have not been considered as the timing of their submittal does not comply with 37 CFR 1.97.

As a second matter, particular attention is drawn to *Golden Bridge Technology Inc. v. Nokia Inc., 87 USPQ2d 1049 (Fed. Cir. 2008)* wherein it was established that appellant cannot raise new arguments on appeal without appropriate justification. In the cited case, the Federal Circuit also refused to remand the case back to the lower court to further consider the new arguments. The examiner brings attention to this case because appellant raised several new arguments in the appeal brief filed on 6/30/08 which the examiner respectfully submits should not be considered by the Board because appellant has failed to submit any appropriate reasons why these arguments and evidences were not entered earlier for consideration by the examiner prior to appeal. Attention is also drawn *KSR International Co. v. Teleflex Inc., 82 USPQ2d 1385 (U.S. 2007)* which establishes among other things how to approach deciding whether or not a claimed invention is obvious. *KSR v. Teleflex* clearly states that a person of ordinary skill is not an automation but rather is someone having ordinary creativity and common sense. The examiner will show that appellant treated a person of ordinary skill as an automation rather than someone having ordinary creativity and common sense, thus appellant's approach towards determining obviousness with respect to the current application is clearly flawed.

As a final matter, the examiner believes that before addressing the actual rejection providing a summary of the art used in the rejection of the claims would be beneficial. The primary reference, Kessler, relates to the field of encrypting data and transferring files within a peer-to-peer environment (col 1, lines 6-8). The users of Kessler's invention each obtains a proprietary client software which facilitates file transfers between users by registering with an application server 200 from whom the

client software is obtained (col 4, lines 33-46). The software itself has included therein a public key, a secret key, encryption and decryption algorithms, and obfuscation and de-obfuscation algorithms, wherein the keys are inaccessible to the user (col 4, lines 58-62 and col 8, lines 50-56). These keys and obfuscation and de-obfuscation algorithms are obfuscated and/or encrypted within the proprietary client software for additional security (col 8, lines 62-65). To transfer a file between a first and second user, a track key TK, is used to encrypt the particular file for transfer (col 5, lines 38-47). TK itself is transferred from one user to the other using a key-encrypting-key protocol (col 5, lines 38-48). TK was generated either by one of the users or by application server 200 (col 2, lines 29-32 and col 5, lines 29-38). At the receiving computer, encrypted TK is extracted using a secret key corresponding to the public key used to encrypt TK (col 6, lines 52-57). TK is then used to decrypt the particular file that was exchanged (col 6, lines 52-59).

Okada discloses techniques for protecting data transfer between a host unit/access apparatus and a data recording apparatus (col 1, lines 29-34). Note that a data recording apparatus is an apparatus for digital recording and playback while an access apparatus could be a personal computer (col 1, lines 6-14). Note that one cannot playback a file without accessing the file, thus one skilled in the art should appreciate that both the access apparatus and data recording apparatus could both refer to personal computers. As such, one skilled in the art having ordinary creativity and common sense would have recognized that Okada's teachings are also applicable towards protecting data transfer between two separate computers. Of particular interest is that Okada teaches secure transfer of a file between a recording apparatus and an access apparatus by encrypting the file with a contents key and encrypting the contents key using at least a session key (col 5, lines 32-57). The cited portion also discusses how after transferring the encrypted content, the encrypted contents key

is decrypted using at least the session key and the transferred content is decrypted using the decrypted contents key. In summary, with respect to Okada's invention, since the same session key is used in both the encryption and decryption of the contents key, Okada teaches a key-encrypting-key method wherein the key used to encrypt the contents/file key is a symmetric/common key.

Shen Orr discloses of a variable security mechanism for securing digital content in which a single security mechanism is not used for all content (abstract). Shen Orr taught various methods of obfuscation to protect at least a portion of software code/descrambler (p16, line 3-p17, line 3 and p24, lines 17-19). The particular obfuscation technique used is chosen based on a variable parameter such as a hardware or software identifier, i.e. target id (p9, line 19-p10, line 2). Encryption of the software, obfuscation of the software, compiling of the software, and sending of the software in Shen Orr's invention all takes place in a single application builder program (Fig 1; Fig 4A-4B; and p34, lines 10-31). Note also that Shen Orr considers encryption of data to be a type of obfuscation technique since it hides at least a portion data (p23, line 17-p34, line 2).

LeVine's invention relates to protecting digital information from unauthorized use (paragraph 3). In particular he teaches an obfuscation technique which involves scrambling/interleaving/scattering a key within the instruction stream of a program (paragraphs 12, 21, 23, 26, and 78).

Appellant's arguments will now be addressed. Note that the examiner will use the same headings as appellant so that the reader may more easily follow which traversal is meant to address which particular argument in the filed appeal brief (hereinafter AB#, where # refers to the page number of the appeal brief filed on 6/30/08). It is noted that the claims all stand or fall together since

appellant used claim 1 as a representative claim for the arguments presented. In traversal, the examiner will also use claim 1 as a representative claims.

Elements are selectively extracted and recombined in a way that changes the principles of operation of Kessler.

Appellant argues in AB14 that the rejection apparently considers the client computer of "User 1" in the peer-to-peer network that provides access to a file as the application program provider of claim 1. Appellant further states that if the rejection relies upon some other interpretation of the application program provider based on Kessler, such an interpretation directly contradicts the teachings of Kessler so cannot stand.

The examiner respectfully submits that the rejection never stated or implied that the client computer of User 1 was equivalent to the claimed application program. The Final office action on page 7 (OA 11/26/07) cited Kessler showing the existence of a proprietary client software having embedded decryption algorithm and explained that a person of ordinary skill in the art should understand that *all programs start out as source code and when the source code is compiled, the resulting software contains instruction streams…the fact that proprietary software exists implies that a reference to a decryption algorithm was received and used to create the proprietary software*. If the rejection stated or implied anything was equivalent to the claimed application program, it would be the application builder used to create Kessler's proprietary client software. Note that as per MPEP 2112, the express, implicit, and inherent disclosures of the prior art reference may be relied upon in the rejection of claims under 35 USC 102 or 103.

The examiner explained in the rejection on page 7(OA 11/26/07), why the existence of the proprietary software implied the existence of some application program provider or application builder used to create the proprietary client software, i.e. created by compiling source code. The rejection further recognized that the Kessler does not explicitly state that the receiving, creating, applying, scrambling, and sending steps were done on a single application program provider/program builder, but further relied upon Shen Orr's teachings to show that it would have been obvious to do all these stated steps to create a program on a single application builder/application program provider (see Final Office action, p11). One way of doing this based on Shen Orr's teachings is by modifying the application server 200 disclosed by Kessler so that it not only provides/sends the proprietary software program to the users, but it is also used to build the proprietary software program. Instead of addressing the actual rejection, appellant misconstrues the rejection to instead say that the computer of User 1 was stated as being the claimed application program provider—the rejection stated no such thing. The receiving, creating, applying, scrambling, and sending steps as recited in claim 1 essentially describe the creating and sending of a particular obfuscated key decryption program on a single application provider, thus it is unclear how appellant can confuse the computer of User 1 of Kessler as being equivalent to the claimed application program when neither Kessler nor the rejection discussed the computer of User 1 as having created the proprietary client software. The rejection clearly recognizes that the users obtained the proprietary client software from application provider 200 during a registration step (see for example p8, lines 3-4 of the Final Rejection, which cites portions of Kessler discussing this).

Further, contrary to appellant's arguments, interpreting whatever application builder used to create the proprietary client software of Kessler as being equivalent to the claimed application

program provider would not contradict the teachings of Kessler since all programs start out as source code and must be created, i.e. by compiling the source code. The examiner also notes that appellant has failed to provide any evidence that interpreting the application builder used to create the proprietary client software as the claimed application program provider contradicts Kessler's teachings. The arguments of counsel cannot take the place of evidence in the record. In re Schulze, 346 F.2d 600, 602, 145 USPQ 716, 718 (CCPA 1965); In re Geisler, 116 F.3d 1465, 43 USPQ2d 1362 (Fed. Cir. 1997). Kessler clearly states that the users registers with a an application server to download the proprietary client software (col 4, lines 33-46), thus appellant stating that the computer of User 1 is the application program provider clearly is illogical since the computer of User 1 does not create the proprietary client software and the rejection never stated that it did.

The examiner further notes that this is the first time appellant has presented arguments stating that the appellant thought the examiner had stated that the client computer of User 1 of Kessler is the claimed application program provider. The examiner in rejecting the claims attempted to be as clear with his explanations as possible, however, recognizes that what may be clear to the examiner might not be clear to other readers. Had appellant earlier presented this argument, it would have alerted the examiner to appellant's confusion and the examiner could have provided further clarification prior to appeal so that appellant would not be making clearly erroneous arguments. As per *Golden Bridge Technology Inc. v. Nokia Inc., 87 USPQ2d 1049 (Fed. Cir. 2008),* the examiner respectfully submits that the argument that the computer of User 1 being different from the claimed application program provider of claim 1 should not even be considered by the Board since appellant failed to present the argument for the examiner's consideration prior to appeal and failed to present any reason why it was not earlier presented for the examiner's consideration. Further, any arguments which stems from

appellant misinterpreting the computer of User 1 as being the application program provider of claim 1 should also not be considered for similar reasons.

On AB15, paragraph 1, appellant argues that to suggest the method of claim 1, the rejection must rely upon processes performed on the client computer of User 1 as this is the system that provides the file and reliance upon operations performed on any other entity **as was done in the rejection** changes the principle of operation of Kessler. The examiner respectfully disagrees.

The first thing the examiner notes with respect to the above argument is that appellant recognized that the examiner did not rely upon operations performed on the client computer of User 1 in the rejection of claim 1—appellant clearly states in the first paragraph of AB15 that the rejection relied upon operations performed on other entities, thus it is unclear how in the argument presented on AB14 and already addressed above, appellant could then confuse that the rejection in any way shape or form implied that the client computer of User 1 was the claimed application program provider.

Further contrary to appellant's argument, reliance upon operations performed on any other entity as was done in the rejection does not change the principles of operation of Kessler. The examiner notes that appellant has not provided any evidence that relying on operations performed on other entities would change the principle operations of Kessler. The arguments of counsel cannot take the place of evidence in the record. In re Schulze, 346 F.2d 600, 602, 145 USPQ 716, 718 (CCPA 1965); In re Geisler, 116 F.3d 1465, 43 USPQ2d 1362 (Fed. Cir. 1997). For this reason alone, the examiner respectfully submits that appellant has failed to overcome prime facie case of obviousness.

Further, as shown above, the examiner had relied upon the implied application builder of Kessler to show an application program provider and relied upon the additional teachings of Shen Orr

to show that it would have been obvious to perform each of the recited steps of claim 1 in a single application builder/program provider (for example by having application server 200 of Kessler also be an application builder). The examiner further explained why the existence of the proprietary client software implied the existence of the application program provider used to create the client software. Use of an application builder as the application program provider would not change the principle operation of Kessler of a secure peer-to-peer file transfer system (col 1, lines 6-8) since the proprietary client software has to be created somehow. Nothing argued by appellant thus far overcomes the prima facie case of obviousness set forth by the examiner. At best all of appellant's arguments thus far have been based either purely on arguments without evidence or based on rejections and statements never made or implied in the Final Office action, thus appellant has failed to overcome prima facie case of obviousness.

The rejection relies upon components on two different systems which teaches away from the common entity of the claims

In the section spanning pages 15-16 of the appeal brief, appellant makes several incorrect statements and then presents arguments based on those incorrect statements. The first incorrect statement made by appellant is that Kessler taught that key TK is generated on the client computer of User 1. This is not entirely correct. Kessler taught that TK is generated either on the client computer of User 1 **or by application server 200** (col 2, lines 29-32 and col 5, lines 29-38). Recall that application server 200 was also where the users downloaded the proprietary client software (col 4, lines 44-46, i.e. application server could then be viewed as an application program provider since it provides the client program to registered users). Since both TK and the client software could be

downloaded from the same server, one skilled having ordinary creativity and common sense would have recognized that one could download TK along with or as a part of the proprietary client software.

Appellant then states that Kessler further taught that preferably, encrypting operations on key TK were performed on the client computer of User 1. The examiner respectfully submits that "preferably" is not the same thing as "must". Kessler clearly states that TK could instead be encrypted by application server 200 (col 5, lines 37-38). As discussed above already, it would have been obvious based on the teachings of Kessler and Shen Orr to modify the application server 200 to also be an application program builder/provider. Based on Kessler and Shen Orr's teachings cited, it would have been obvious to have TK be encrypted at the application server/application builder/application program provider of Kessler and Shen Orr's teachings for the reasons discussed in the Final Rejection. It is also noted that appellant apparently only considered the teachings of Kessler alone (select teachings at that) in presenting arguments in AB15-16, which is insufficient to overcome prima facie case of obviousness since the rejection of the claims were not made based on Kessler's teachings alone. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

Appellant states in AB15 that the rejection relies upon a secret key SK2 which is only available on the client computer of User 2 as the first cryptographic key of claim 1 and a key TK that is generated and encrypted only on the client computer of User 1 as suggesting the second cryptographic key of claim 1. Appellant states that both the first and second cryptographic keys are on the application program provider while the rejection relies on elements on two different entitles. The examiner respectfully submits that appellant is incorrect. First, as shown above already, the

second cryptographic key TK is not necessarily generated and encrypted only on the client computer of User 1. The examiner discussed already how it could instead be generated and encrypted in the application server 200, i.e. the claimed application program provider. The examiner further submits that applicant has done a piece-meal analysis of the references and of rejection of claim 1. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

The examiner agrees with appellant that the examiner relied on SK2 as the claimed first cryptographic key. SK2 is embedded within the clients software via obfuscation and/or encryption (col 4, lines 56-62 and col 8, lines 62-65), which meets the claimed criteria of receiving, on an application program provider, a reference to a decryption algorithm and a first cryptographic key. Page 7 of the Final office action explains how all software starts out as source code. One cannot embed the secret/first key in the client software in the manner disclosed by Kessler if one did not receive the first cryptographic key to embed. The secret key SK2 also meets the claimed criteria that the key decryption program be configured to perform decryption algorithm for said first decryption key. Note that the client software disclosed by Kessler is a key decryption program because it has built-in decryption algorithms (col 8, lines 50-53) and the secret key SK2 is used to by the key decryption program/client software to perform the decryption algorithm (col 10, lines 61-62). The examiner then went on to discuss how the first cryptographic key disclosed by Kessler differed from the claimed first cryptographic key in that Kessler's first cryptographic key (see p8 of the Final office action, paragraph starting on line 5). Specifically, it was recognized by the examiner that whereas the invention as claimed in claim 1 uses a symmetric key system to encrypt and decrypt the second

cryptographic key, Kessler uses a public key system so that a public key was used to encrypt TK/second cryptographic key while using a secret key SK2 to decrypt TK. However, the examiner went on to point out that Okada taught that use of at least a session key to both encrypt and decrypt a second/file/content key was known in the art (see p8 of the Final office action, paragraph starting on line 5). The examiner stated in the paragraph spanning pages 8-9 of the Final Office action that based on this teaching by Okada, it would have been obvious to one skilled in the art to modify Kessler's invention so that rather than use a public/private key pair to encrypt the second key TK, a symmetric key system was used instead. One would do this by modifying SK2 to be a symmetric key and use SK2 to both encrypt and decrypt TK. Appellant's arguments focus solely on Kessler, whereas the rejection of claim 1 discussed modifying Kessler's invention to use a symmetric key-encrypting-key system based on Okada's teachings. Because appellant's arguments are based on a piece-meal analysis of the references and does not address the actual rejection made, it is respectfully submitted that the rejection be maintained. Note that in failing to address the actual rejection made, appellant's argument fails to comply with 37 CFR 1.111(b).

Appellant, in the last paragraph of AB15, states again that according to the rejection, User 1 is equivalent to the application program provider based on the encryption of key TK that is done on the client computer of User 1. The examiner has already addressed above how the rejection never stated that User 1 or the computer of User 1 was equivalent to the application program provider, thus will not repeat the traversal here for brevity sake. The examiner had also already addressed how TK was not necessarily encrypted in the client computer of User 1, thus will also not repeat the traversal here for brevity sake. However, the traversals already discussed above apply here also.

Appellant recognizes in the paragraph spanning AB15-16 that the rejection requires a modification to Kessler, but states that the modification requires making SK2 (which was available only to the computer of User 2) available to User 1, because otherwise what the rejection identifies as the first and second cryptographic key are not available in on a common entity as recited in claim 1. Appellant argues that making secret key SK2 of User 2 available to User 1 destroys the intent of Kessler that secret key SK2 is only available to User 2 and would require a change in the principles of operation of Kessler, which is forbidden by MPEP 2143.01. The examiner respectfully disagrees that the proposed modification as set forth by the Office would change the principle of operation of Kessler. Note that the Office action does not propose changing Kessler's SK2 so that it is available to both Users 1 and 2, only that it is available for use by both the client software of both Users 1 and 2. Note that even when Kessler uses a public/private key pair, neither keys are available or accessible to the users of the client computers since it is embedded within the client software (col 4, lines 58-62). Even if one were to replace the public/private key pair of Kessler with a symmetric key as per Okada's teachings so that a symmetric key was used to encrypt TK, one skilled having common sense and ordinary creativity would have recognized that one would still want to make the symmetric key used in the resulting key-encrypting-key system inaccessible to everyone and everything except the proprietary client software itself as Kessler had done with the public/secret key of his unmodified invention. As such, Kessler's principle operation of a secure peer-to-peer file transfer system (col 1, lines 6-8 and 16-19) would not change since the modified secret key would still be secure and would still be usable to securely transfer a key TK from one user's computer to another so that both computers could come to an agreement on a common file encryption key.

The rejection relies upon processes on multiple different systems which teaches away from the common entity of the claims

Appellant alleges in the paragraph spanning AB15-16 that the rejection confuses process performed on different entities and attempts to hide the confusion by making assertions that are incorrect and not based on any teachings of or suggestion of Kessler. As an example, appellant quotes the rejection as saying "This implies that when the proprietary software was created, not was the source code to the decryption algorithm received" *[sic]*. Appellant states that while the statement may be correct; it is not relevant unless there is some suggestion as recited in claim 1 that a key decryption program was created on an application program provider. Appellant states there is no teaching cited that the source code was created on the client computer of User 1 that has been identified in the rejection as the application program provider. Again, the examiner respectfully notes that the rejection never stated that the client computer of User 1 was ever interpreted to be the application program provider. Appellant in making arguments based on this incorrect assumption fails to comply with 37 CFR 1.111(b) since appellant fails to address the actual rejections made.

As discussed above already, the existence of the proprietary client software in Kessler's invention implies an application builder was used to create the software from source code (this was discussed on page 7 of the Final Office action). The application builder, which one skilled should recognize could be incorporated into application server 200 (based on Shen Orr's additional teachings) of Kessler is what the examiner is interpreting as the claimed application program provider. Applicant's argument fails to address the actual rejection made.

As to why the statement made by the examiner that software are created from source code on an application program provider is relevant to claim 1, the first and second limitations recited in claim

1 implies the steps necessary to create a software (i.e. the claimed key decryption program) from a source code. The first claimed step--receiving, on an application program provider, a reference to a decryption algorithm and a first cryptographic key can be interpreted as receiving, at an application program provider/builder, a source code having a decryption algorithm and a key used in the decryption algorithm. The source code is the reference to a decryption algorithm since the client software created in Kessler's invention has necessary decryption algorithms (col 8, lines 50-53). The second step--creating, on said application program provider, a key decryption program comprising an instruction stream, said decryption program configured to perform said decryption algorithm for said first cryptographic key could reasonably be interpreted to mean creating the executable program on the application program provider/builder using the source code containing the decryption algorithm and first cryptographic key received (i.e. by compiling the source code). The created software would be the proprietary client software of Kessler, which as discussed above already, is configured to perform a decryption algorithm using a first cryptographic key, i.e. to recover encrypted key TK (col 10, lines 59-67). Note that all software programs comprise instruction streams. Appellant stated that the statements made by the examiner are relevant if there was some suggestion as recited in claim 1 that a key decryption program was created on an application program provider. Since the examiner has shown that there is suggestion as recited in claim 1 that a key decryption program was created on an application program provider, the relevancy of the statement should be apparent.

Appellant argues in AB18 that Kessler does not teach any decryption program was created on the client computer and was instead created elsewhere and supplied to the client computer as part of a registration process with a server. Again, the examiner respectfully submits that the rejection never stated that the proprietary client software was created by the user's computer. It is unclear how

appellant has so misconstrued the rejection made by the Office. The rejection clearly recognizes that the client software was created elsewhere and provided to the user as part of a registration process (see Final Office action p7-p8, line 3). The sections cited by the Office action clearly shows the client software of Kessler which contains a decryption program (col 8, lines 50-53) being downloaded by the users as part of a registration process from an application server 200, thus it is unclear how the Office action in any way shape or form implied that it was the client computers that could be interpreted as application program providers. Again the examiner notes that this was the first time appellant has presented arguments based on this misinterpretation of the Office action for the examiner's consideration, thus the examiner respectfully submits that the Board should not even consider any arguments based on this incorrect interpretation of the Final Office action since appellant has not presented any reasons why these arguments were not presented for the examiner to consider earlier, see *Golden Bridge Technology Inc. v. Nokia Inc., 87 USPQ2d 1049 (Fed. Cir. 2008).*

In the last paragraph on AB18, appellant argues that to teach or suggest the element of claim 1, the rejection must cite creating a key decryption program for key SK2 on the client computer of User 1, which the rejection identifies as the application program provider. Again, appellant's argument is based on clearly erroneous interpretation of what was stated in the Final Office action. How such a mistake could be made by appellant is unclear since, as already discussed above, in the first paragraph on AB15, appellant apparently recognizes that the Office did not rely on processes performed on the client, thus could not have relied upon the computer of User 1 as the claimed application program provider. Appellant seems to be contradicting himself since appellant states that the Office action relied upon the computer of User 1 as the application program provider, yet the cited portion of AB15 provides evidence that appellant recognized that the Office did no such thing.

In AB19, appellant argues that the rejection reduces the explication claim limitation to a gist that something does the sending and confuses peer-to-peer file sharing with the action of providing the proprietary client software. Appellant states that the key TK of Kessler is used in the peer-to-peer file sharing but the client software that is considered the instruction stream of claim 1 is not sent anywhere by the client system of User 1. The examiner respectfully submits that the rejection cited column 4, lines 44-46 and column 8, lines 50-51of Kessler as meeting the limitation of sending said key decryption program, not merely a sending of something. The cited portions clearly shows the client proprietary software being sent to a user's computer system from an application server 200 as part of a registration process. It is appellant that has confused not only Kessler's teachings, but also the rejection made by the examiner. The portions cited by the examiner has nothing to do with peer-to-peer file sharing except that it shows the software being used in the peer-to-peer file sharing being sent from the application server 200 to a user's computer system. How this even comes close to the examiner reducing the claimed limitation to "the gist" of something does the sending is unclear. As discussed above already, based on Kessler and Shen Orr's teachings the application server 200/appliacation builder could be considered the claimed application provider, thus the claimed limitation as a whole and the claim as a whole were fully considered by the examiner.

Appellant argues that claim 1 recites that the obfuscated key decryption program is sent from the application program provider while the decryption program in the client software package of Kessler is not provided or sent by the client computer of User 1 but was received in the registration process from a server and the decryption program was not used by User 1 in the process of providing a file. This argument is again not reflective of the actual rejection made, thus fails to comply with 37 CFR 1.111(b). Both the Office and appellant are in agreement that the client computers receive a

software package (i.e. the proprietary client software) from a server computer (i.e. application server 200), the software package containing a decryption program. This clearly teaches the limitation of sending, from said application program provider, said key decryption program as asserted by the Office (see p8 of Final Rejection, lines 3-4 and p11, first paragraph).

Kessler taught away from obfuscating key TK

In the second paragraph of AB20, appellant argues that Kessler expressly taught away from obfuscating key TK when that key was transferred by User 1. Appellant argues TK is only taught as being encrypted when transferred. The basis of this argument apparently is that Kessler knew that obfuscation existed, but didn't obfuscate TK, thus he teaches away from it. The examiner respectfully disagrees. The reference showing that it knows of obfuscation but not applying obfuscation to TK is not the same as the reference teaching away from obfuscation—the examiner is unaware of any precedence in case law or in the MPEP which would make appellant's opinion with respect to this matter correct. An explicit disclosure by Kessler that obfuscation of TK is undesirable would be an example of evidence of teaching away from obfuscating TK, but no such evidence exists. In fact, one skilled in the art should understand that obfuscation of information merely refers to making information hidden or difficult to decipher, thus encryption of TK itself could broadly and reasonably be interpreted as one form of obfuscation. Cited reference Shen Orr even discloses of one obfuscation scheme which uses encryption for obfuscation (p33, line 17-p34, line 2), thus appellant's argument that Kessler expressly teaches away from obfuscation of TK is clearly not correct since encryption (broadly, but reasonably interpreted) is one form of obfuscation and as applicant points out, TK was encrypted by Kessler when transferred.

The processes associated with secret key SK2 are not on the application provider as characterized by the rejection.

In the last paragraph of AB20, appellant argues SK2 is used only by the client computer of User 2 and the cited processes are performed on the client computer of User 2, which is not what the rejection considers the application program provider, the client computer of User 1. Again, the examiner respectfully points out that the rejection never considered the client computer of User 1 as the application program provider. Appellant's arguments fails to comply with 37 CFR 1.111(b) since it fails to address the actual rejection made.

Whatever application builder that is used to create the client software is considered the application program provider and when viewed with the additional teachings of Shen Orr, the application server 200 of Kessler could be modified so that it is also the application builder/application program provider as already discussed numerous times above. Further, as already discussed above, based on Okada's teachings, it would have been obvious to modify Kessler's invention so that a symmetric key was used to encrypt TK by modifying SK2 to be a symmetric key. Modifying SK2 in this manner would make it so that SK2 was not merely used for decrypting TK, but also to encrypt TK, thus SK2 would no longer be used merely by the client computer of User 2. The examiner further submits that based on the argument just traversed, appellant appears to have once again done a piece-meal analysis of the rejection and the references since appellant apparently only considered Kessler's teachings alone rather than the teachings of all the references as a whole as detailed in the Final Rejection. One cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871

(CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986).

In the first paragraph of AB21, appellant states that the rejection selectively extracts pieces from various parts of Kessler and recombines them in a way that changes the principle of operation of Kessler with no rationale for the selective extraction. Specifically, appellant argues the rejection selectively extracts (1) a piece of Kessler that is performed on an undefined entity (the generation of the proprietary software); (2) a piece of peer-to-peer file transfer process on the client computer of User 1 (the generation and encryption of key TK); and (3) a key SK2 and processes performed on the client computer of User 2. The examiner respectfully submits that the so called selective extraction did not take place.

As pointed out above numerous times, appellant has clearly misunderstood the rejections made in the Final Office action and has misunderstood Kessler's invention. Appellant focuses only upon certain aspects of Kessler's invention while ignoring his teachings as a whole. Appellant had stated that generation and encryption of TK, what is considered equivalent to the claimed second key, can only take place in the client computer of User 1. The examiner showed this to be incorrect since Kessler also allows it to be created and encrypted by the application server 200 from which the proprietary client software was downloaded (col 5, lines 36-38). As such, the process that appellant has stated the examiner extracted, i.e. (2) the peer-to-peer file transfer process on the client computer of User 1 (the generation and encryption of key TK), in fact was not extracted from the client computer of User 1. Instead, this process took place at the application server 200--which as already pointed out above, based on the combined teachings of Kessler and Shen Orr, could be viewed as the claimed application program provider.

With respect to (3) a key SK2 and processes performed on the client computer of User 2, as pointed out above already, the rejection recognized that there were differences between SK2 of Kessler's invention and the claimed first cryptographic key. Specifically, based on Kessler's teachings alone, appellant is correct in that SK2 would only exist in the client computer of User 2 since a public key method was used in Kessler's key-encrypting-key protocol. However, the rejection also relied upon the teachings Okada, which showed that it would have been just as obvious to instead both encrypt and decrypt a content/file key using a symmetric key system (col 5, lines 32-57) rather than a public key system as done by Kessler. In ignoring the teachings of Okada, appellant has done a piece-meal analysis of the references and has failed to address the actual rejection made. Because appellant did not address the actual rejection made, the argument fails to comply with 37 CFR 1.111(b). Further, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. See *In re Keller*, 642 F.2d 413, 208 USPQ 871 (CCPA 1981); *In re Merck & Co.,* 800 F.2d 1091, 231 USPQ 375 (Fed. Cir. 1986). Because of these numerous errors by appellant, the rejection should be maintained since appellant's arguments fail to overcome prima facie case of obviousness as set forth in the Final Rejection.

In the second and third paragraph of AB21, appellant clearly recognizes that in the references as a whole must be considered. As shown above, appellant has clearly failed to do this and in doing so assumes that it was the examiner who mischaracterized Kessler's teachings when clearly it was appellant who mischaracterized not only Kessler's teachings, but the rejections made in the Final Office action. Appellant states that the rejection requires changes to the principles of operation of Kessler, but appellant has failed to provide any proof of this. The arguments of counsel cannot take the place of evidence in the record. In re Schulze, 346 F.2d 600, 602, 145 USPQ 716, 718 (CCPA

1965); In re Geisler, 116 F.3d 1465, 43 USPQ2d 1362 (Fed. Cir. 1997). Kessler's principle of operation is a system which provides for secure transfer of files in a distributed environment (col 2, lines 16-19), none of the modifications to Kessler's invention proposed by the Office action based on the teachings of Okada, Shen Orr, and LeVine changes this principle of operation.

The rejection mischaracterizes the teachings of Okada

Appellant argues the rejection mischaracterizes the teachings of Okada. Appellant argues that Okada stated that the encryption was with a host ID, the session key and the first drive ID and that Okada did not teach that the content key was decrypted using the session key as stated in the rejection, but rather was decrypted using the drive key. The examiner respectfully disagrees. Okada teaches multiple embodiments of his invention and in some of the embodiments the contents key could be encrypted using more than one key, thus would necessitate be decrypted using more than one key (col 5, lines 33-57; col 9, lines 21-25; and col 10, lines 45-52—note that at least one of those keys is a session key as discussed in the Final Office action). This does not change the fact that use of a session key to both encrypt and decrypt a contents key was taught by Okada. The portion cited by the examiner clearly shows an embodiment of Okada's invention where a session key is used to both encrypt and decrypt the contents keys. What appellant has done is point to one section of Okada which discusses use of a session key (along with other keys) used to encrypt the contents key (col 9, lines 22-26), then point to another section (col 10, lines 39-42) which doesn't have anything to do with decryption to undo the encryption done with the session key discussed in column 9, lines 22-26. This sort of analysis of Okada by appellant is about as useful and just as ridiculous as if someone

were to point to a section of Okada which discusses encryption and then point to just Okada's patent number and then say "clearly Okada only teaches encryption, but not decryption since the patent number doesn't say anything about decryption". As evidenced by the above portions of Okada cited by the examiner, Okada does in fact teach encryption of a contents key using a session key and decryption of the encrypted contents key using the same session key. The portion cited by appellant (col 10, lines 39-42) which discusses decryption of the session key using a drive key is to undo encryption using the drive key as discusses in column 9, lines 47-50, not decryption to undo the encryption of the contents keys that was encrypted using the session key as discussed in column 9, lines 22-26. It was appellant who mischaracterized Okada's teachings, not the examiner. Clearly appellant has failed to consider the reference as a whole since appellant so severely mischaracterized Okada's teachings.

The combination changes the principle of operation of Kessler so is not appropriate.

Appellant argues beginning on the lat paragraph of AB23 that if the modification of Kessler (i.e. based on Okada's teachings) reduces the security level taught by Kessler, the modification changes the principles of operation and so would not be appropriate. Appellant states that the rejection does not even consider the potential reduction in security and relies only on performance as a rationale for modifying Kessler. Appellant states that Okada, taken as a whole taught the level of security was sufficient when a common storage are on disk drive was used and the rejection ignores that the encrypted contents keys is stored in a storage section 150 of a disk drive by Okada. Appellant states that the encrypted contents key of Okada is not incorporated into any instruction stream and is not sent anywhere, rather the key is taught by Okada as being maintained on a disk drive, therefore

taken as a whole, Okada taught that this level of security was suitable when both entities access the same disk drive and so taught away from use of this level of security for any transfer over a network. The examiner respectfully disagrees.

As discussed above, Kessler's principle of operation is to provide a system for securely transferring files between client computers (col 2, lines 16-19). Okada's principle of operation is to provide a technique which can protect data from illegal accessing with (col 5, lines 1-8). Okada's field of invention relates to techniques for protecting data from illegal access when the data is transferred between a data recording apparatus and an access apparatus (col 1, lines 6-14). In the cited section of Okada in column 1, he discusses that a recording apparatus is for example an apparatus for playback of music, video, and the like. An access apparatus could be a personal computer. A person of ordinary skill in the art should appreciate that one cannot playback data without accessing it, thus a recording apparatus could also be an access apparatus, thus could also be a personal computer. As such, a person of ordinary skill in the art having common sense and ordinary creativity would have recognized that Okada's teachings could also be adapted to protect data from illegal access when data is transferred between two personal computers, i.e. such as in the case with Kessler's invention. Appellant arguing that Okada's teachings could not be incorporated into Kessler's invention shows that appellant has treated a person of ordinary skill as an automation having no common sense and no creativity.

As to the argument that incorporating Okada's teachings within Kessler's invention would reduce the security level and change the principle of operation, the examiner respectfully submits that Kessler's principle of operation is a system for security transferring files between computers (col 2, lines 16-19). Kessler does not define how much security is needed for his invention to consider that

secure transfer of files is taking place. Even if one were to reduce the security at some level, as long as there still is some security for the file transfer, Kessler's principle of operation has not changed. Since encryption of the file being transferred still occurs in Kessler's modified invention, there is still secure file transfer between two computers. A person of ordinary skill in the art should understand that speed of operation and security are often conflicting goals in computing system. Specifically, the more securely one make a computing system, the slower it typically operates while the faster one makes a computing system, the less secure it tends to be. However, balancing security with speed for various circumstances by sacrificing one for the other has been something that has always taken place in the art and one skilled in the art having ordinary creativity and common sense would have recognized that in a peer-to-peer file sharing environment, high level of security is not always desirable; sometimes a high speed of transfer is more desirable than high security. Consider that Napster is the assignee of the Kessler reference. As one skilled in the art should recognize, Napster was a company which provided software for peer-to-peer sharing of files among multiple users. Speed was more often a concern for peer-to-peer file sharing using Napster's software rather than security, so even if there may be some (not all) reduction in security by incorporating Okada's teachings within Kessler's invention, Kessler's principle of operation of providing a secure peer-to-peer file sharing environment has not changed. It would only change if security was totally eliminated, however, clearly the modifications proposed by the Office action does not totally remove security from the peer-to-peer file transfer.

Further, consider that key technology is not the only way of providing security--one skilled in the art should have realized this. In Kessler's unmodified invention, even though he uses a public/private key pair to encrypt/decrypt TK, the key pair is inaccessible to the user (col 4, lines 58-

62). One skilled having common sense would have recognized that if one were to swap out Kessler's key-encrypting-key system with Okada's so that a symmetric key was used to encrypt TK instead, one can still maintain a relatively high level of security by maintaining Kessler's teachings of not letting the users of the client computer have access to the symmetric key used to encrypt TK. One skilled would have also recognized that part of what makes a public key system more secure as compared to a symmetric key system is that public keys tend to be much larger than symmetric keys, but because of the large size processing using these large keys tend to be slower. A person skilled in the art having common sense and ordinary creativity would have recognized that one could still have a reasonably high level of security using a symmetric key-encrypting-key system as taught by Okada either by making the symmetric key used to encrypt TK larger than normal size or by doing as Okada did and using other keys along with a session key in the encryption of a content/file key (col 5, lines 32-57). Note that claim 1 as recited does not forbid other use of other keys other than a first and second cryptographic keys. One skilled in the art having common sense and ordinary creativity would have recognized that there are numerous way Okada's teachings could have been incorporated into Kessler's invention so that security is not reduced. However, as pointed out above, even if security was necessarily reduced by incorporating Okada's teachings, this does not mean that Kessler's principle of operation was changed as long as there is still some security provided for the file transfer.

As per the argument that the rejection does not even consider the potential reduction in security and relies only on performance as a rationale for modifying Kessler, the examiner has shown above that the examiner did consider the potential reduction in security and recognized that it would not have changed the principle of operation of Kessler. Further, the rejection did not rely only upon

performance as a rationale for modifying Kessler based on Okada's teachings. In the Final Rejection in the paragraph spanning pages 8-9, the rejection clearly states that "Another rationale for why it would have been obvious to modify Kessler's invention in the manner discussed using Okada's teachings is that the simple substitution of Okada's key encrypting key methodology within Kessler's invention would do no more than yield the predictable result to a track key (TK) being encrypted and decrypted using a single first cryptographic key rather than use of an asymmetric key pair to encrypt and decrypt TK." This rationale was based on *KSR v. Teleflex* and appellant has failed to even address this rationale in presenting arguments as to why it would not have been obvious to combine Kessler and Okada's teachings.

As per the argument that Okada, taken as a whole taught the level of security was sufficient when a common storage are on disk drive was used and the rejection ignores that the encrypted contents keys is stored in a storage section 150 of a disk drive by Okada that the encrypted contents key of Okada is not incorporated into any instruction stream and is not sent anywhere, rather the key is taught by Okada as being maintained on a disk drive, therefore taken as a whole, Okada taught that this level of security was suitable when both entities access the same disk drive and so taught away from use of this level of security for any transfer over a network, the examiner respectfully notes appellant has treated one of ordinary skill as an automation rather than someone having ordinary creativity and common sense as required by *KSR v. Teleflex*. As discussed above, one skilled in the art having ordinary creativity and common sense when considering Okada's teachings as a whole would have recognized that his teachings could have been adapted towards providing security for file transfer between two computers such as in the case with Kessler's invention. The rejection even discussed how this could be done (see Final Office action, p8). Applicant states that Okada does not

incorporate an encrypted content key into any instruction stream and the key is not sent anywhere, but again applicant has done a piece-meal analysis of the references by considering only Okada's teachings by itself rather than what the teachings of the references as a whole would have made obvious to one of ordinary skill in the art. Encrypted content keys being incorporated into instruction streams was discussed as obvious over LeVine's additional teachings, not Okada (see Final Office action, p10, last two paragraphs). The encrypted content keys being sent from one computer to another was obvious based on Kessler's teachings of sending TK from one computer to another (col 5, lines 43-47). Applicant states that Okada taught away from use of the security level used in his invention for transfer of files over a network, but failed to provide any evidence of this, thus it would appear that is argument is based on appellant's opinion alone. The arguments of counsel cannot take the place of evidence in the record. In re Schulze, 346 F.2d 600, 602, 145 USPQ 716, 718 (CCPA 1965); In re Geisler, 116 F.3d 1465, 43 USPQ2d 1362 (Fed. Cir. 1997).

In the last paragraph of AB24 and first paragraph in AB25, appellant argues that the rejection throwing away the public-private key pairs of Kessler and using the session key of Okada in their place ignores the environment in which Okada taught such use was appropriate and changes the principles of operation of Kessler as a session key would not be suitable for use in the proprietary software package provided to each client as the same session key would not help to differentiate between users as in the unique key pairs used by Kessler. The examiner respectfully disagrees. The examiner had discussed already why Okada's teachings taken as a whole would have been applicable also for security file transfer between two computer systems, for example, as done by Kessler, thus the environment in which Okada taught use of his keys was not ignored. The examiner respectfully submits that appellant in insisting that Okada's teachings could only be used in securing

data between a drive and a computer, ignores the teachings of Okada taken as a whole and treats one of ordinary skill in the art as an automation rather than someone having common sense and ordinary creativity as required by *KSR v. Teleflex*. One of ordinary skill in the art would have sufficient creativity to be able to adapt Okada's teachings beyond just securing files between a drive and a personal computer because as discussed above, Okada's field of invention deals with securing file transfers between a recording apparatus and access apparatus (col 1, lines 6-14), both of which could be computers. Further one skilled in the art should recognize that it has long been known in the art that one can access, from one computer, the drive of another computer over a network connection, thus when viewed in light of this knowledge of one of ordinary skill in the art, one skilled having common sense and ordinary creativity would have recognized that Okada's teachings could have been applied towards security file transfer between two computers in a network.

As per the argument that use of a session key in place of a public-private key pair would change the principle of operation of Kessler, the examiner has already addressed above why this argument is incorrect since Kessler's principle of operation is providing a system for secure file transfers between two computers (col 2, lines 16-19) and the modification proposed by the Office action based on Okada's teachings still provides for this.

As per the argument that use of a session key in Kessler would not be suitable for use in the proprietary software package provided to each client as the same session key would not help to differentiate between users as the unique key pairs used by Kessler, the examiner first notes that this is the first time appellant has presented this argument for consideration. As per see *Golden Bridge Technology Inc. v. Nokia Inc., 87 USPQ2d 1049 (Fed. Cir. 2008)*, the examiner respectfully submits that the Board should not even consider this argument since appellant has failed to provide

appropriate justification why this argument was not presented for consideration prior to appeal when the examiner had discussed modifying Kessler using Okada's teachings in by replacing the public-private key pair using a session key since the very first Office action. Even if this argument was considered, the examiner respectfully submits that it is not persuasive because Kessler does not state anywhere that use of the unique key-pairs is required nor use of the unique key pair to differentiate between users is required for his invention to properly function as a system for secure file transfer between two computers. When a user registers with an application server 200, the user downloads to his/her computer system the proprietary client software for use in the secure peer-to-peer file transfer (col 4, lines 44-46 and col 8, lines 50-51). A person of ordinary skill should recognize that each user could be uniquely identified using other means than just a unique key pair. For example, a unique user id and password could be assigned to each user during the registration process. Kessler does not discuss anywhere that the unique key pair is required to uniquely differentiate between the users in his system and that it is required for his invention to work, thus the argument that swapping it out for a session key as per Okada's teachings would change the principle operation of Kessler's invention has no base in fact and appears to be based on appellant's opinion alone. The arguments of counsel cannot take the place of evidence in the record. In re Schulze, 346 F.2d 600, 602, 145 USPQ 716, 718 (CCPA 1965); In re Geisler, 116 F.3d 1465, 43 USPQ2d 1362 (Fed. Cir. 1997).

Appellant argues in the second paragraph of AB25 that the modification of as session key for the key pair would reduce the security level since use of a common session key would allow any party that had the session key to decrypt the file rather than a single user as in Kessler. Again, it is noted that this is a new argument never before presented prior to appeal, thus as per see *Golden*

Bridge Technology Inc. v. Nokia Inc., 87 USPQ2d 1049 (Fed. Cir. 2008), the examiner respectfully submits that the Board should not even consider this argument since appellant has failed to provide appropriate justification why this argument was not presented for consideration prior to appeal. Even if it was considered, the argument is incorrect. As noted above, in Kessler's unmodified invention which uses a public/private key pair, the key pair is not accessible to the user (col 4, lines 58-62) and Kessler does not disclose use of the key pair to differentiate the users as appellant is arguing. One skilled in the art would have recognized that Kessler's invention could be applicable for securing transfer of files between registered users in a peer-to-peer environment, thus it may not be necessary to prevent registered users from being able to decrypt any file from any other registered user as long as it prevents access by non-registered users. Since the keys are embedded in the client software which could only be obtained by registering (col 4, lines 44-62), it is not necessarily undesirable to modify Kessler's invention so that it has a slightly reduced level of security. An invention which allows any registered user to decrypt files from other registered users but prevents non-registered users from decrypting the file would still provide a system for secure peer-to-peer file transfer as desired by Kessler (col 2, lines 16-20), thus his principle of operation would not be changed. Kessler does not disclose anywhere that it is required in his invention that only a single user be able to decrypt the file.

The Advisory Action statements rejecting this argument contradict the rejection.

Appellant argues on AB26 that the rejection relies upon replacing the keys used in the encrypting and decrypting key TK with a different key, whoever the advisory action stated the contrary. Appellant argues that the advisory action makes it clear that the public/private key pair is essential so agrees with appellant. Appellant argues that the comments in the advisory action fail to

address the substance in the remarks and instead argue about key TK which was not even at issue. The examiner respectfully disagrees that the Advisory action contradicts the rejection and that the examiner ever agreed that the public/private key pair is essential to Kessler's invention.

The argument submitted after Final Rejection that the examiner was responding to in the Advisory stated that the public and private key pair was needed to make the file transfer work and any other key combination would break Kessler. The examiner sees now that appellant was attempting to argue that any other key in place of the public and private key pair would break Kessler, however, appellant's argument at the time was not clear and the examiner had taken it to mean that appellant had thought that Kessler's invention did not use any other keys other than public and private key pair. In response to this, the examiner pointed out in the Advisory action that TK was also used in the file transfer process of Kessler's invention along with the public/private key pair. Kessler's unmodified invention using a public/private key pair was never anything the examiner disagreed with and as discussed above, the rejection recognized this as a difference between Kessler's invention and appellant's claimed invention (see Final Rejection p8). However, as discussed above, the rejection went on to explain how use of the public/private key pair was not essential to Kessler's principal of operation of a system for secure file transfer between two computers (col 2, lines 16-19) since a symmetric key could be used instead as taught by Okada (see Final Office action, p8). The Advisory action does not contradict the rejection since it was responding to an argument made by appellant that was not clear at the time. The examiner recognizing that Kessler's unmodified invention uses a public/private key pair is not agreement with appellant that use of a public/private key pair is required for Kessler's principle of operation to be maintained. The examiner has discussed numerous times

above why use of a session key as taught by Okada in place of a public/private key pair would not change Kessler's principle of operation.

Appellant argues in the next to last paragraph in AB27 that Kessler was familiar with both public key encryption and symmetric encryption and taught which encryption was best in the different circumstances, thus is further evidence that the modification in the rejection changes the principles of operation of Kessler. The examiner respectfully disagrees. Kessler knowing of both public key encryption and symmetric key encryption and choosing to use public key encryption in certain circumstances is not evidence of anything. Kessler does not state anywhere that use of a public key system in his invention is essential or required for the operations of his invention. The examiner has discusses numerous times above already how using a symmetric key system in place of public key system would not change Kessler's principle of operation, thus appellant's argument is without any basis in fact. Kessler summarizing an embodiment of his invention by stating that two different encryption technologies are used to provide the secure peer-to-peer environment is not the same thing as two different encryption technologies are required to provide peer-to-peer environment. One skilled should also appreciate that even with use of symmetric keys, several types of encryption technologies exists based on symmetric keys (i.e. DES, AES, block encryption, stream encryption, etc. are all different types of encryption technologies which uses symmetric keys). As such even if one used a symmetric key in place of the public/private key pair, it is still possible to provide a peer-to-peer environment based on two or more encryption technologies using symmetric keys, i.e. one type of symmetric encryption technology to encrypt TK and a separate type of symmetric encryption technology to encrypt files using TK. Note also that Okada also taught encrypting the contents key using multiple keys which would require decrypting the contents key multiple times (col 9, line 16-col

10, line 53), thus it would also have been obvious to modify Kessler's invention based on Okada's teachings by encrypting TK multiple times including using of a first cryptographic session key while keeping Kessler's asymmetric key-encrypting-key technology in the modified invention.

The combination with Shen Orr is based on mischaracterizations and so violates the as a whole requirement.

Appellant argues in AB29 that Shen Orr is concerned with obfuscating a "descrambler/player" and does not teach obfuscation of a key decryption program as recited in claim 1. The examiner respectfully disagrees. The "descrambler/player" disclosed by Shen Orr can be considered a key decryption program as claimed. The key decryption program as claimed in claim 1 comprises an instruction stream and is configured to perform said decryption algorithm for said first cryptographic key. In other words, the key decryption program is software which uses the first cryptographic key to perform decryption according to a decryption algorithm. The descrambler disclosed by Shen Orr is software which descrambles/decrypts digital content to a clear format with a key (p15, lines 14-16). All software programs comprises an instruction stream, thus the descrambler/player that appellant recognizes as being obfuscated by Shen Orr clearly meets the requirement of "obfuscation of a key decryption program" as recited in claim 1. Further, even if it was not a key decryption program as claimed (though it is), one skilled would have enough common sense and creativity to recognize that the descrambler/player of Shen Orr is software, thus since Shen Orr teaches obfuscation of software, one could apply his teachings to any other type of software and obfuscate those software. For example, one could apply Shen Orr's teachings to Kessler's client software and obfuscate it to obtain an obfuscated key decryption program as claimed. Appellant failing to recognize this shows that

appellant has treated one of ordinary skill in the art as an automation rather than someone having ordinary creativity and common sense as required by *KSR v. Teleflex*.

Appellant argues in AB29 that both Kessler and Okada taught there was no need to modify Kessler so that the key was obfuscated. The examiner respectfully disagrees. Neither Kessler nor Okada ever stated any such thing and appellant has failed to provide any evidence where either reference state that obfuscation of a key is unnecessary. Appellant states that both Kessler and Okada taught that the key relied upon in the rejection was only encrypt, not obfuscated—this appears to be the basis of appellant's insistence that Kessler and Okada teaching that obfuscation of the key is unnecessary. However, as discussed above already, Kessler knowing about obfuscation and not obfuscating the key is not evidence that he decided that it was unnecessary to obfuscate the key. Shen Orr clearly discusses that it was there was an unmet need in the art of secure content delivery which provides variable security mechanisms (p6, lines 9-26). Incorporating Shen Orr's teachings within Kessler's invention so that the keys are not only encrypted, but also obfuscated using various other obfuscation techniques (p6, lines 27-33) as per Shen Orr's teachings would meet this long felt need in the art. Kessler's invention as discussed above already also relates to secure content delivery. Note also that Shen Orr considers encryption to be a type of obfuscation technique since encryption hides at least a portion of the obfuscated data (p23, line 17-p34, line 2). As such, appellant stating that by only encrypting the key, Kessler decided that obfuscation of the key is unnecessary gives too narrow a definition of what obfuscation is as would have been understood by one of ordinary skill in the art. While use of variable security determined by a target ID within Kessler's invention was made obvious over Shen Orr's teachings (see discussion in Final Office action p9-10), particular obfuscation by scrambling the key relied upon into the instruction stream

using a code obfuscation method was made obvious over LeVine's additional teachings (see discussion on page 10 of Final Office action).

Appellant argues in AB29 that the rational for the modification demonstrates that the modification to Kessler changes the principles of operation of Kessler. The examiner respectfully disagrees. Appellant has also failed to provide any evidence or rationale as to why modifying Kessler's invention in the manner discussed in the rejection based on Shen Orr's teachings would change Kessler's principle of operation, thus fails to overcome prima facie case of obviousness. The arguments of counsel cannot take the place of evidence in the record. In re Schulze, 346 F.2d 600, 602, 145 USPQ 716, 718 (CCPA 1965); In re Geisler, 116 F.3d 1465, 43 USPQ2d 1362 (Fed. Cir. 1997).

Appellant argues on AB29-30 that the rejection again confuses the proprietary software tools provided by Kessler with the transfer of a file over the peer-to-peer network. Appellant quotes the rejection as stating:

> At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to further modify Kessler's invention using Shen Orr's teachings by obfuscating Kessler's proprietary client software before sending it to the client....

Appellant states that the keys that are relied on in the rejection are used in the peer-to-peer file transfer and the computer system of User 1 as cited as the application program provider of claim 1. The examiner respectfully submits that appellant's argument that the rejection confuses the teachings of Kessler is once again based on misinterpretation of the rejection. As explained above numerous times, the rejection never stated that the computer system of User 1 was cited as the application program provider of claim 1. How appellant can misinterpret the rejection in this manner is unclear since appellant has admitted to recognizing that the rejection did not cite the computer system of

User 1 as the claimed application provider, see as evidence the first paragraph in AB15 where appellant clearly states that other entity than the computer system of User 1 was relied upon. Since the basis of appellant's argument is clearly erroneous, appellant's argument is traversed.

Appellant argues in AB30 that comments concerning protection of the transfer of the proprietary software package of Kessler demonstrate that Kessler is being modified in ways that goes against the express teachings of Kessler. The examiner respectfully disagrees. As evidenced by the above quoted section, the comments did not concern modifying Kessler's invention so that the transfer of the proprietary software package was protected. Note that various components of the software package such as keys and various algorithms are secured against user access in Kessler's invention (col 4, lines 58-62 and col 8, lines 62-64). The securing of these components has nothing to do with securing the software package for transfer, but rather is for securing against user access even after the software was transferred to the user. The rejection proposed strengthening the manner in which Kessler secured these various components from user access based on Shen Orr and LeVine's teachings, not against transfer of the software package. Appellant's arguments fails to address the actual rejection made, thus fails to comply with 37 CFR 1.111(b).

The remaining arguments are towards allowance of the dependent claims due to dependency on the independent claims. However, because all of appellant's arguments for the independent claims were traversed, the dependent claims are also not allowable.

As can be seen from the discussion above, appellant's arguments failed to overcome the prima facie case of obviousness as set forth in the Final Office action for several reasons. Appellant either presented argument which are new and should not be considered by the Board at all or set forth arguments based on flawed understanding of the art and of the rejection as set forth in the Final

Office action. The manner in which appellant analyzed the art and the rejection was also defective. Among the manners in which appellant's analysis was defective included treating one of ordinary skill in the art as an automation rather than someone having ordinary creativity and common sense, doing a piece-meal analysis of the art rather than considering what the teachings of the references as a whole would have made obvious to one of ordinary skill in the art, failing to address the actual rejection made by the Office, and presenting counsel's opinions as the basis for arguments rather than evidence. Because all of appellant's arguments have been traversed, it is respectfully submitted that the rejections as set forth in the Final Office action be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Ponnoreay Pich

/Ponnoreay Pich/

Examiner, Art Unit 2135

Conferees:

/KimYen Vu/

Supervisory Patent Examiner, Art Unit 2135

/Hosuk Song/

Primary Examiner, Art Unit 2135